FIG. 1
(PRIOR ART)

PLAIN TEXT

IP — 110

L_0 | R_0 ← K_1 — 120

122 ⊕ 121 f

$L_1 = R_0$ | $R_1 = L_0 \oplus f(R_0, K_1)$ ← K_2

122 ⊕ 121 f

$L_2 = R_1$ | $R_2 = L_1 \oplus f(R_1, K_2)$ ← K_3

122 ⊕ 121 f

$L_3 = R_2$ | $R_3 = L_2 \oplus f(R_2, K_3)$

$L_{14} = R_{13}$ | $R_{14} = L_{13} \oplus f(R_{13}, K_{14})$ ← K_{15}

122 ⊕ 121 f

$L_{15} = R_{14}$ | $R_{15} = L_{14} \oplus f(R_{14}, K_{15})$ ← K_{16}

122 ⊕ 121 f

$L_{16} = R_{15}$ | $R_{16} = L_{15} \oplus f(R_{15}, K_{16})$

IP^{-1} — 130

CIPHER TEXT

FIG. 2
(PRIOR ART)

FIG. 3
(PRIOR ART)

FIG. 4
(PRIOR ART)

DATA   KEY

~400

INITIAL PERMUTATION
UNIT

MULTIPLEXER 1	MULTIPLEXER 2

~410   ~420

COMBINATION LOGIC
UNIT 1   ~430

COMBINATION LOGIC
UNIT 2   ~440

~450   ~460

REGISTER 1	REGISTER 2

FINAL PERMUTATION
UNIT   ~470

CIPHER TEXT

FIG. 5A
(PRIOR ART)

a_0

b_0

UNROLLED LOOP
CIPHER FUNCTION UNIT

K_m

f_m

K_n

f_n

8 rounds

8 rounds

CLK

A

B
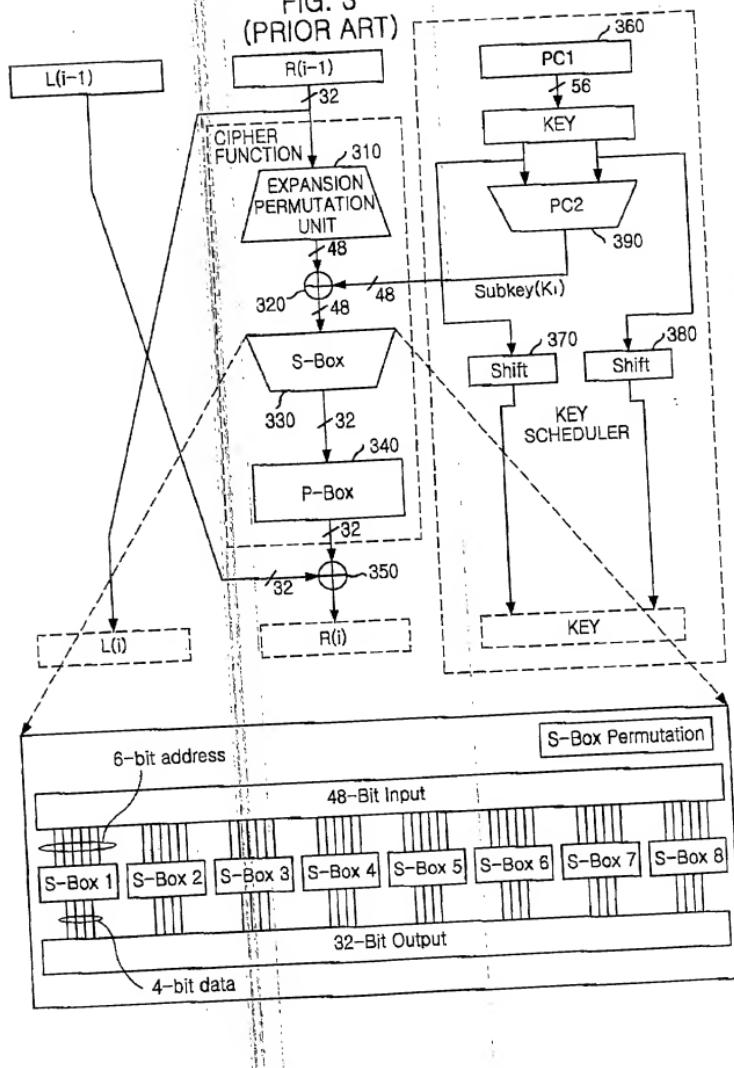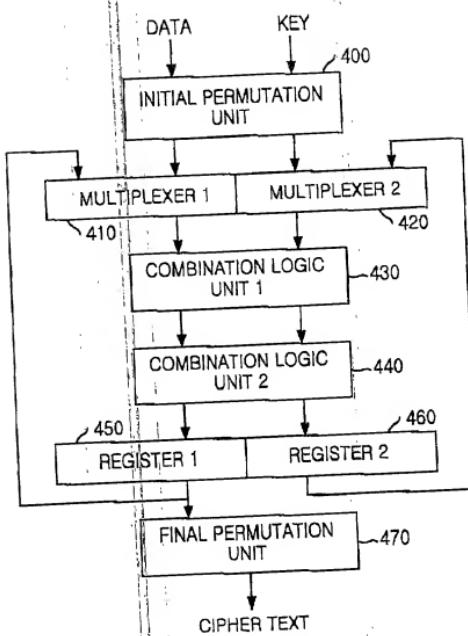
ⓕ CIPHER FUNCTION UNIT
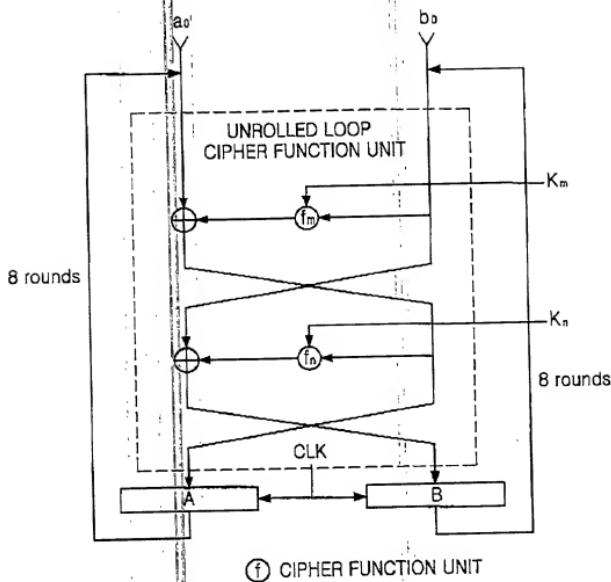
FIG. 5B
(PRIOR ART)

FIG. 6
(PRIOR ART)

$R_A (=R_{2i-3})$

$R_B (=R_{2i-2})$

32

32

f_m

610 EXPANSION PERMUTATION UNIT

48

620 ⊕ 48 ← $K_m (=K_{2i-1})$

48

S-BOX PERMUTATION UNIT

630   640

32

P-BOX PERMUTATION UNIT

32

32

⊕ 650

32

$R_{2i-1} = R_{2i-3} \oplus f(R_{2i-2}, K_{2i-1})$

f_n

32

EXPANSION PERMUTATION UNIT

48

⊕ 48 ← $K_n (=K_{2i})$

S-BOX PERMUTATION UNIT

32

P-BOX PERMUTATION UNIT

32

⊕ 32

32    $R_{2i} = R_{2i-2} \oplus f(R_{2i-1}, K_{2i})$

$R_C (=R_{2i-1})$

$R_D (=R_{2i})$
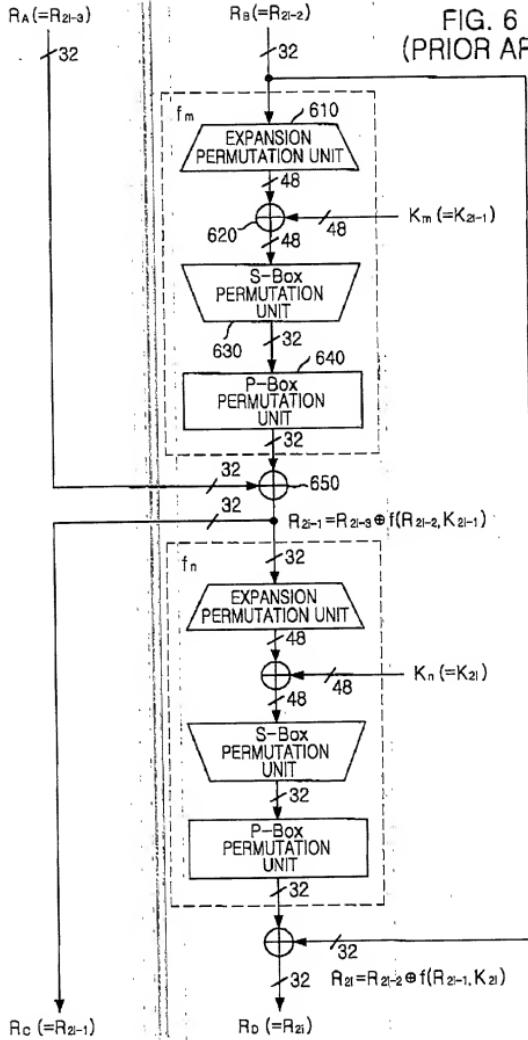
FIG. 7
(PRIOR ART)
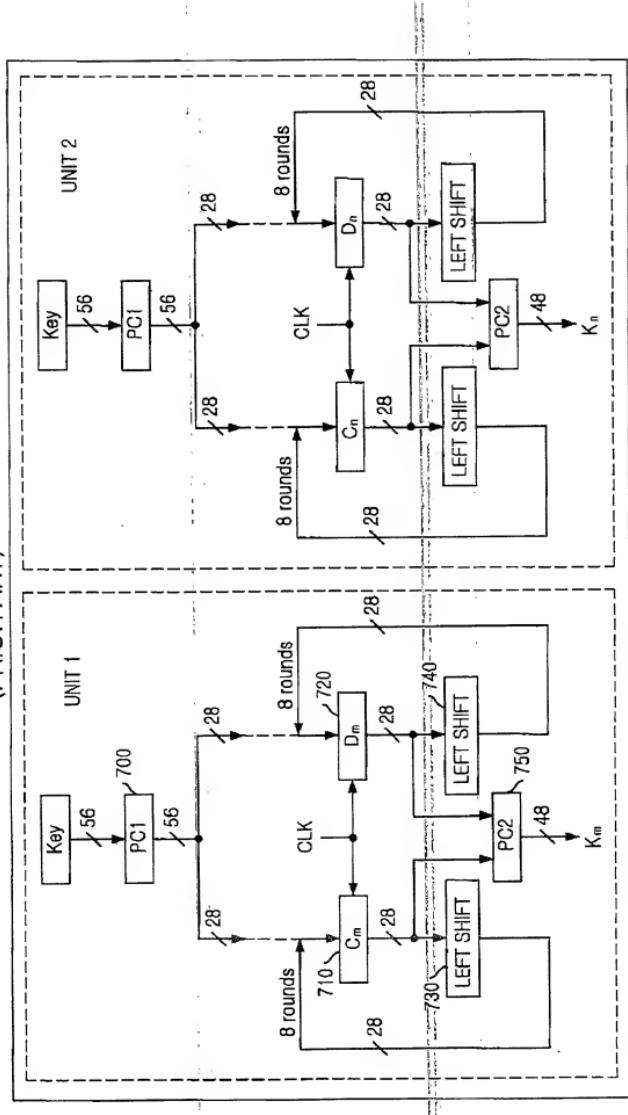
FIG. 8

Round	S_m	TS_m	D_m	TS_n
1(P_0)	3	1	+1	2
2(P_1)	4	4	+2	6
3(P_2)	4	8	+2	10
4(P_3)	3	12	+2	14
5(P_4)	4	15	+2	17
6(P_5)	4	19	+2	21
7(P_6)	4	23	+2	25
8(P_7)	2*(1)	27	+1(0)	0
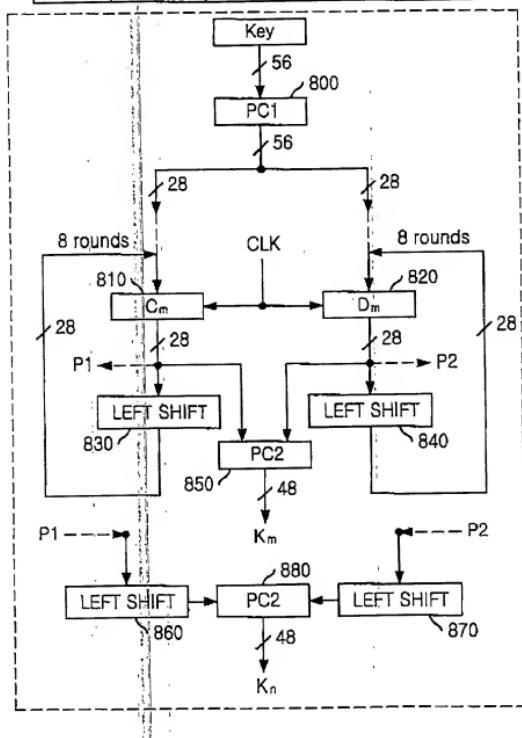
FIG. 9

Round	S_n	TS_n	D_n	TS_m
1(P_0)	4	2	−1	1
2(P_1)	4	6	−2	4
3(P_2)	4	10	−2	8
4(P_3)	3	14	−2	12
5(P_4)	4	17	−2	15
6(P_5)	4	21	−2	19
7(P_6)	3	25	−2	23
8(P_7)	2	0	−1	27

FIG. 10

FIG. 11

Gather Data Formatting

Input Byte Stream

8Clock Cycles

I7
I6
I5
I4
I3
I2
I1
I0

· · ·

CLK1 → IBR(L) — 1110

CLK1 → IBR(R) — 1120

A₁

Time Multiplexed Cipher Function

B₁

32

32

32

K_B

48

48

K_A

1132 ⊕

f_B

f_A

⊕ 1135

32

1131

1134

32

CLK1 → A0 — 1133

~CLK1 → B0

1136

32

32

~CLK1 → OBR(L) — 1140

~CLK1 → OBR(R) — 1150

Scatter Data Formatting

· · ·

Output Byte Stream

8Clock Cycles

O7
O6
O5
O4
O3
O2
O1
O0
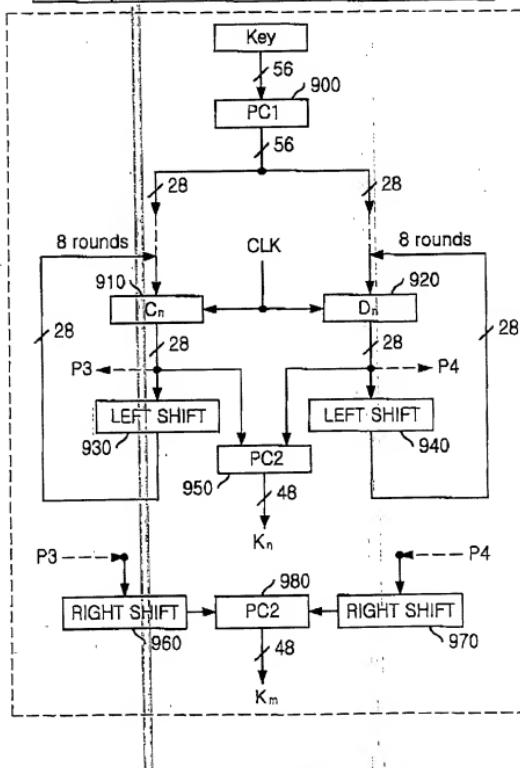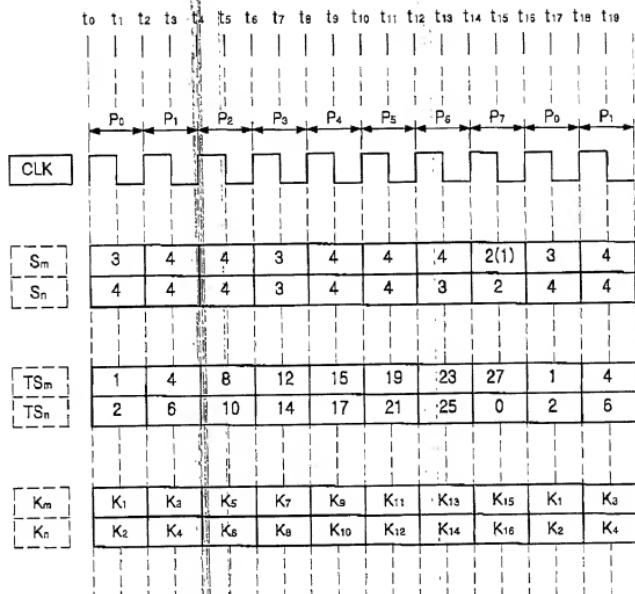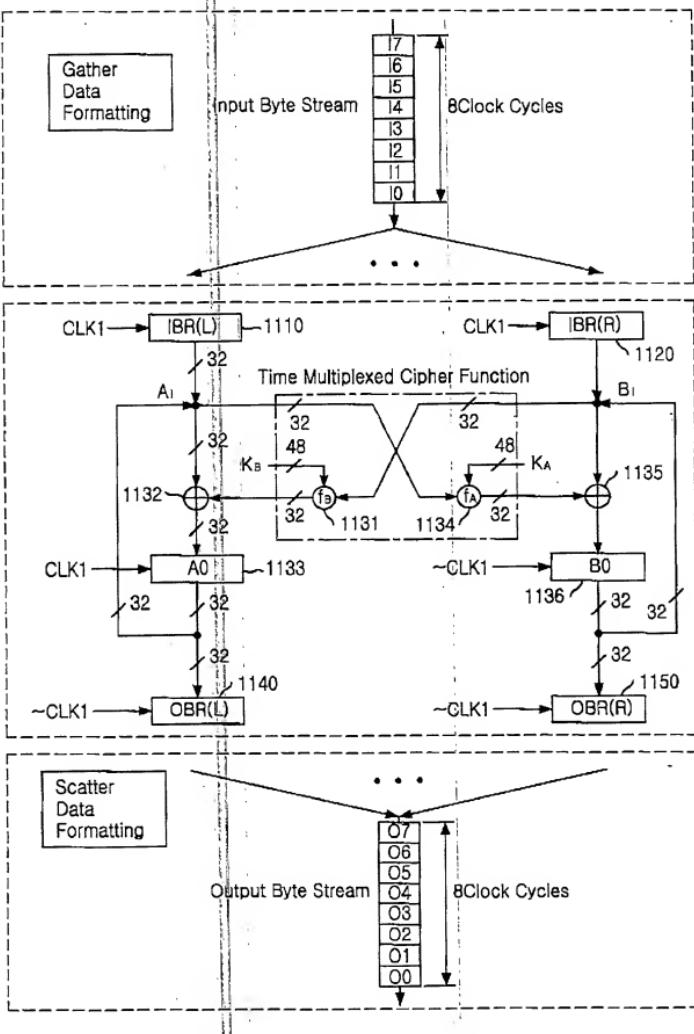
FIG. 12
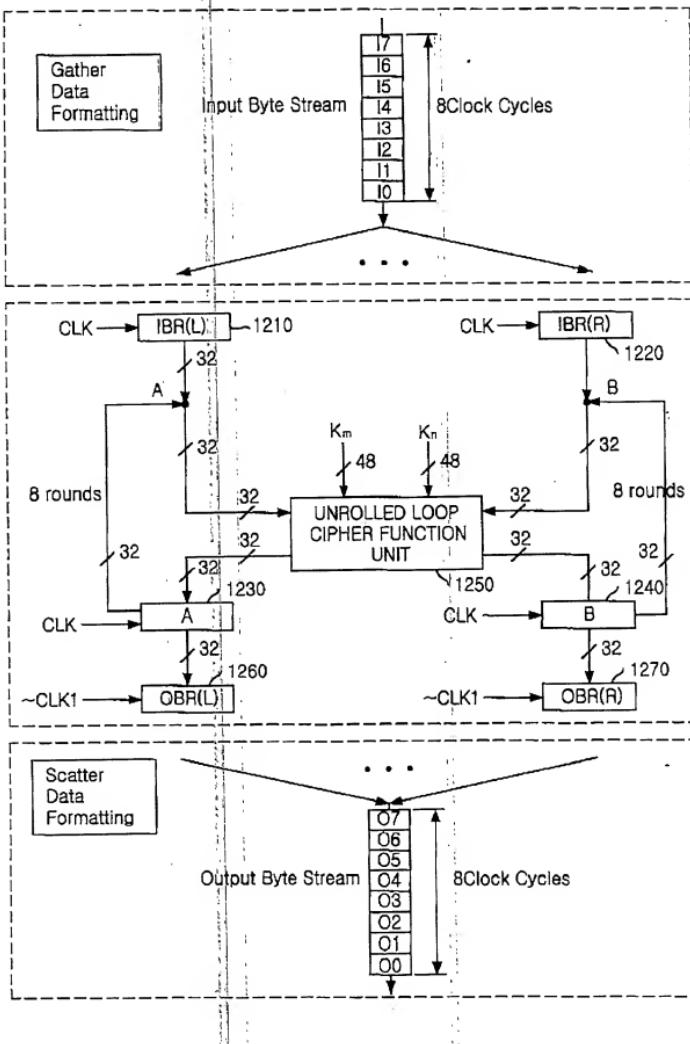
FIG. 13
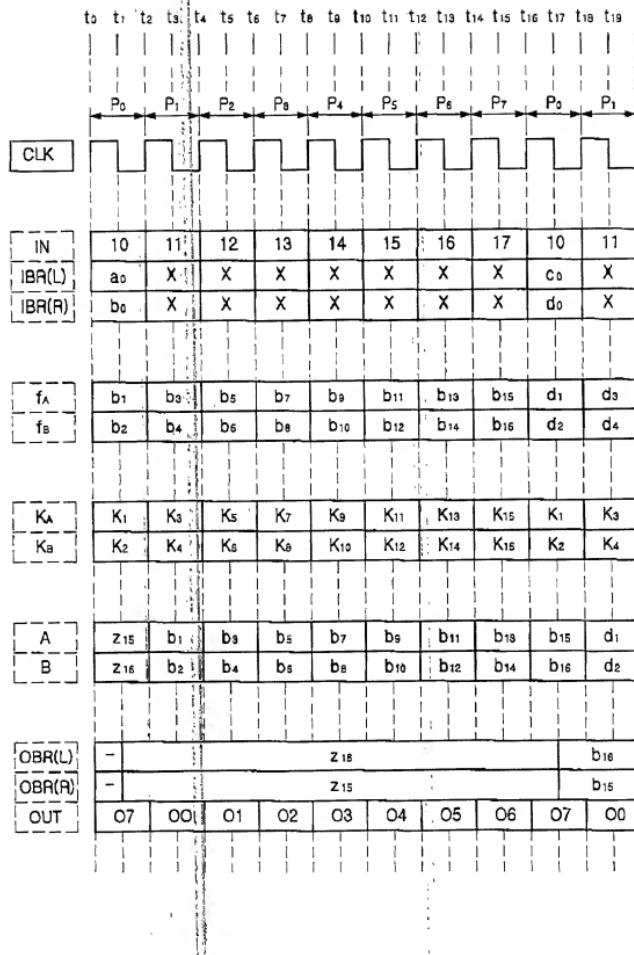
FIG. 14

Traditional 16 Round DES

(1) No Latency Hiding (Latency=32, Throughput=1/32)

←	32Cycle	→	←	32Cycle	→			
IN	16-DES	OUT	IN	16-DES	OUT	IN	16-DES	OUT
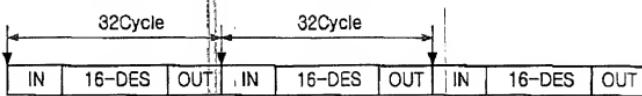
(2) 2-Stage Macro Pipeline (Latency=32, Throughput=1/24)

←	24Cycle	→	24Cycle	→	24Cycle	→	
IN	16-DES	OUT					
		IN	16-DES	OUT			
				IN	16-DES	OUT	
					IN	16-DES	
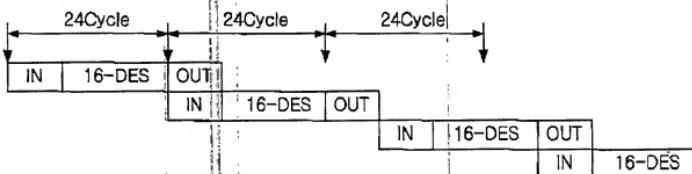
(3) 3-Stage Macro Pipeline (Latency=40, Throughput=1/16)

16Cycle	16Cycle	16Cycle	16Cycle	16Cycle
IN	idle	16-DES	OUT	idle
	IN	idle	16-DES	OUT	idle
		IN	idle	16-DES	OUT	idle
			IN	idle	16-DES	OUT	idle
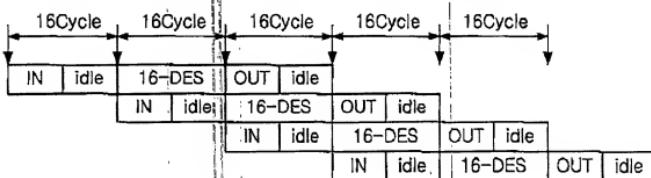
8Round DES (Loop Unrolled Cipher function & Time Multiplexed Cipher Function)

(4) 3-Stage Macro Pipeline (Latency=24, Throughput=1/8)

8Cycle	8Cycle	8Cycle	8Cycle	8Cycle
IN	8-DES	OUT		
	IN	8-DES	OUT	
		IN	8-DES	OUT
			IN	8-DES	OUT
				IN	8-DES	OUT